

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In Re JETBLUE PRIVACY LITIGATION

This Document Relates To:
All Actions

Master File No. 03-CV-4847

**FIRST AMENDED CLASS
ACTION COMPLAINT**

Jury Trial Demanded

Plaintiffs, by their undersigned counsel, for their First Amended Class Action Complaint, allege the claims set forth herein.¹ Plaintiffs' claims as to themselves and their own actions, as set forth in ¶¶ 9-21 herein, are based upon their personal knowledge. All other allegations are based upon information and belief and are made pursuant to the investigations of counsel. Based upon such investigation, Plaintiffs believe that substantial evidentiary support exists for the allegations herein and that such allegations are likely to have additional evidentiary support after a reasonable opportunity for further investigation and/or discovery.

¹By filing this First Amended Class Action Complaint, Plaintiffs take no position, other than on behalf of themselves and the members of such Class as may be certified by this Court in this action, on any proceedings before the Judicial Panel for Multidistrict Litigation. Nor do Plaintiffs intend to represent any claimant or plaintiff in any case not pending before or properly transferred to this Court. In addition, Plaintiffs, on behalf of themselves and any plaintiff in a related case filed in or transferred to this Court in the future, reserve the right to have any case returned to its transferor forum for trial. This First Amended Class Action Complaint supercedes the Consolidated Class Action Complaint and all other complaints alleging similar claims filed by Plaintiffs in this Court.

NATURE OF THE ACTION

1. This is a privacy class action lawsuit brought under the Electronic Communications Privacy Act – Stored Electronic Communications (“ECPA”), 18 U.S.C. § 2701 *et seq.*, and state and common law. On or about September 19, 2003, Defendant JetBlue Airways Corporation (“JetBlue”) admitted that in September 2002 it gave approximately five million electronically stored passenger names, addresses, phone numbers and itineraries containing highly confidential personal information to Torch Concepts, Inc. (“Torch”), a data mining company, in violation of JetBlue’s own privacy policy as well as federal, state and common law. Acxiom Corporation (“Acxiom”) also provided certain highly confidential information concerning JetBlue passengers to Torch. Through a contract with Defendant SRS Technologies (“SRS”), Torch used that information for a project that had no connection to airline routes, rates or services. Plaintiffs and other Class members had a legally protected privacy interest in the data containing their personal and private information and had an actual and reasonable expectation that someone would obtain their prior authorization and/or consent prior to any transfer of such data.

2. Plaintiffs bring this class action lawsuit on their own behalf and on behalf of a class of persons defined as:

All persons in the United States who provided personally identifiable information to JetBlue Airways Corporation, prior to September 2002 (the “Class Period”), and whose information has been transferred, accessed or otherwise used by JetBlue or another person or entity absent the authorization and/or beyond the consent of the customer (the “Class”).

Excluded from the Class are Defendants; any entity in which Defendants have a controlling interest or that have a controlling interest of Defendants; Defendants’ legal representatives, assigns and successors; any judge or special master assigned to hear any aspect of this litigation, and any member of their immediate families; and, to the extent the class

certification order permits exclusion, all people who submit timely and otherwise proper requests for exclusion from the Class.

3. Defendants, without the prior authorization by Plaintiffs and the other Class members and/or beyond their consent, have engaged covertly in the unauthorized transfer, access or use of stored electronic data containing personal and private information concerning Plaintiffs and members of the Class in violation of federal, state and common law.

4. By secretly transferring, accessing or using customers' electronically stored and highly confidential information concerning JetBlue's customers in contravention of JetBlue's privacy policy, Defendants engaged in serious invasions of privacy and trespasses to property in violation of federal, state and common law.

5. As a result of Defendants' wrongful course of conduct, Plaintiffs have been injured and seek injunctive relief and monetary damages, including punitive damages, to redress Defendants' unlawful activities described herein.

JURISDICTION AND VENUE

6. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2701, *et seq.* This Court also has supplemental jurisdiction over the state and common law claims pursuant to 28 U.S.C. §1367(a).

7. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Defendant JetBlue maintains its principal place of business in this District and/or at all times conducted substantial business in this District.

8. In connection with the acts, transactions and conduct alleged herein, Defendants used the means and instrumentalities of interstate commerce, including the United States' mails and interstate telephone communication.

PARTIES

9. Plaintiff Eric Bauman is a resident of the State of New York. Eric Bauman conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

10. Plaintiff David Block is a resident of the State of Florida. David Block conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

11. Plaintiff Wesley B. Fleet is a resident of the State of Virginia. Wesley B. Fleet conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

12. Plaintiff Susan Florence is a resident of the State of New York. Susan Florence conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, she has had her personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

13. Plaintiff Maurice C. Hakim is a resident of the State of Florida. Marice C.

Hakim conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

14. Plaintiff Thomas Howe is a resident of the State of New Jersey. Thomas Howe conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

15. Plaintiff Sandra Lee is a resident of the State of California. Sandra Lee conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, she has had her personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

16. Plaintiff Kathryn Mortensen is a resident of the State of California. Kathryn Mortensen conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, she has had her personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

17. Plaintiff Elliot B. Richman is a resident of the State of Florida. Elliot B. Richman conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon

information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

18. Plaintiff Deborah Seidband is a resident of the District of Columbia. Deborah Seidband conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, she has had her personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

19. Plaintiff Nicholas R. Singleton is a resident of the State of Florida. Nicholas R. Singleton conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

20. Plaintiff Michael Unger is a resident of the State of Florida. Michael Unger conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon information and belief, he has had his personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

21. Plaintiff Andrea Wittes is a resident of the State of Florida. Andrea Wittes conveyed personally identifiable information to JetBlue during the Class Period in connection with the purchase of one or more tickets for air transportation by JetBlue. Upon

information and belief, she has had her personal and private information unlawfully transferred, accessed or otherwise used by Defendants in violation of federal, state and common law.

22. Defendant Acxiom is a Delaware corporation with its principal place of business at 1 Information Way, Little Rock, AR 72202-2289. Acxiom is a world leader in customer and information management solutions. Upon information and belief, Acxiom conspired with other Defendants to illegally transfer, obtain and provide access to or use confidential information concerning JetBlue's passengers. In furtherance of that conspiracy, Acxiom received certain customer information from JetBlue, which it then transferred to Torch in violation of federal, state and common law.

23. Defendant JetBlue is a Delaware corporation with its principal place of business at 118-29 Queens Boulevard, Forest Hills, New York, 11375. JetBlue is one of the largest passenger carriers in the United States, and had net income of \$54.9 million for 2002. JetBlue conspired with other Defendants to unlawfully transfer, obtain and provide access to or use confidential information concerning its passengers.

24. Defendant SRS is a California corporation with its principal place of business located at 1800 Quail Street, Suite 100, Newport Beach, California 92660. Upon information and belief, SRS conspired with other Defendants to unlawfully transfer, obtain and provide access to or use confidential information concerning JetBlue's passengers. SRS subcontracted with Torch to undertake testing of the consumer profiling study referred to herein as the "Program," without the prior authorization or beyond the consent of the Plaintiffs and members of the Class.

25. Defendant Torch is a Delaware corporation with its principal place of

business located at 4650 Whitesburgh Drive, Suite 101, Huntsville, Alabama, 35802. Torch specializes in information mining and has developed products for the Department of Defense that include data pattern analysis and recognition technology. Torch conspired with other Defendants to unlawfully transfer, obtain and provide access to or use confidential information concerning JetBlue's passengers.

CLASS ACTION ALLEGATIONS

26. Plaintiffs bring this action as a class action, pursuant to Fed R. Civ. P. 23, individually and on behalf of a Class as defined above.

27. The Class is so numerous and geographically dispersed that joinder of all members is impracticable. While the exact number and identity of Class members cannot be ascertained by Plaintiffs at this time, it consists of the approximately 1.5 to 2 million JetBlue customers nationwide who submitted personal and private information to JetBlue that it stored electronically and unlawfully transferred.

28. The number of potential members of the Class is not precisely determined at the present time, but can be established through notice and discovery. The disposition of the Class' claims in this action will substantially benefit both the parties and the Court. The numerosity requirement of Rule 23(a)(1) is, therefore, satisfied.

29. Rule 23 is satisfied because there are questions of law and fact common to Plaintiffs and the Class, which common questions predominate over any individual questions affecting only individual members. Among these common questions of law and fact are:

1. Whether Defendants participated in and/or committed or are responsible for the conduct complained of;

2. Whether Defendants' conduct constitutes the violations of law alleged herein;
3. Whether Defendants devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the Class members Defendants' practice of transferring, accessing or using the personal and private information without Plaintiffs' and Class members' prior authorization or beyond their consent;
4. Whether certain Defendants engaged in deceptive acts and practices in connection with its undisclosed and systemic practice of transferring, accessing or using Plaintiffs' and Class members' electronically stored personal and private information;
5. Whether Defendant JetBlue, through its wrongful course of conduct described herein, breached contracts with Plaintiffs and members of the Class;
6. Whether Defendants' conduct was willful and/or intentional;
7. Whether Defendants were unjustly enriched as a result of their wrongful course of conduct as alleged herein;
8. Whether Plaintiffs and members of the Class have sustained and/or are entitled to damages or are entitled to restitution as a result of Defendants' wrongdoing and, if so, the proper measure and appropriate formula to be applied in determining such damages and restitution; and

9. Whether Plaintiffs and the Class are entitled to an award of statutory damages, compensatory and/or punitive damages and or declaratory, injunctive, and/or other equitable relief.

30. In satisfaction of Rule 23(a)(3), Plaintiffs' claims are typical of the Class members' claims and do not conflict with the interests of any other members of the Class in that Plaintiffs and the Class have all suffered from the same wrongful acts of the Defendants, namely, having their electronic personal and private information surreptitiously and without their authorization or beyond their consent transferred, accessed or used by Defendants. Plaintiffs assert claims that are typical of the claims of the entire Class, all Class members have been subjected to this same wrongful conduct, and the relief Plaintiffs seek is common to the Class.

31. In satisfaction of Fed. R. Civ. P. 23(a)(4), Plaintiffs will protect fairly and adequately the interests of the other Class members. Plaintiffs have no interests that are antagonistic to or that irreconcilably conflict with those of other Class members. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in litigation of this nature to represent them and the Class.

32. A class action is the superior method for the fair and efficient adjudication of this controversy, since joinder of all Class members is impracticable. Plaintiffs are not aware of any potential difficulties in the management of this action as a class action. Furthermore, because the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it prohibitively expensive for Class members to individually redress the wrongs done to them. Thus, because of the nature of the individual Class members' claims in this litigation, few, if any, could otherwise afford to seek legal redress against Defendants for the wrongs complained of herein, and a representative class action is,

therefore, both the appropriate vehicle by which to adjudicate these claims and is essential to the interests of justice.

33. Absent a representative class action, Class members would continue to be injured for which they would have no remedy. Even if separate actions could be brought by individual Class members, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications which might as a practical matter be dispositive of the interests of the other Class members who are not parties to the adjudications, may substantially impede their ability to protect their interests and/or which would establish incompatible standards of conduct for defendants, making certification appropriate under Fed. R. Civ. P. 23(b)(1).

34. Pursuant to Fed. R. Civ. P. 23(b)(2), Defendants have acted and/or refused to act on grounds generally applicable to Plaintiffs and the Class, thereby rendering Class certification and injunctive and/or declaratory relief with respect to the Class as a whole pursuant to this sub-section appropriate as well.

35. A class action regarding the issues in this case creates no problems of manageability. In particular, notice of pendency of this action can be given in a variety of ways, including publication through the Internet and other media.

FACTUAL ALLEGATIONS

JetBlue's Privacy Policy and Acquisition of Personal and Private Information from Plaintiffs

36. Privacy is of paramount importance to consumers. In recognition of this well known fact and in order to encourage customers to share personally identifiable information when making a reservation over the phone or the Internet, JetBlue maintains on its website a clear privacy policy in a claimed effort "to demonstrate our firm commitment to privacy."

According to this policy, JetBlue only uses computer IP addresses to help diagnose server problems, uses cookies to save consumers' names and e-mail so consumers do not need to re-enter such data, and uses optional passenger contact information solely "to send the user updates and offers from JetBlue." Gareth Edmonson-Jones, a spokesman for JetBlue, characterizes JetBlue's privacy policy as "the strongest...in the industry." Based on JetBlue's stated privacy policy, in August 2003, *Consumers Reports* awarded JetBlue a favorable rating for Privacy and Security and Customer Service.

37. JetBlue specifically represents that any financial and personal information collected by JetBlue "is not shared with any third parties, and is protected by secure servers," and also claims to have in place security measures to protect against the loss, misuse and alteration of consumer information under JetBlue's control. Moreover, as to children, JetBlue specifically represents that it does not seek data from children and does not distribute to third parties any personally identifiable information about children without prior parental consent.

38. Despite these self-imposed public assurances that created an obligation under the contract-of-carriage and a duty on the part of JetBlue and persons with whom it did business not to act in derogation of JetBlue's privacy policy and not to share personal and financial information it collected, in September 2002, JetBlue and Acxiom (on behalf of JetBlue) turned over the personal and private information to Torch, as described herein. The personal and private data was contained in JetBlue's electronic communication service and/or remote computing service and concerned approximately 1.5 to 2 million of JetBlue's adult and child passengers that had flown prior to September 2002. This data contained, among other things, passenger names, addresses, and telephone numbers. It also contained information regarding

Class members' itineraries so that Torch could engage in data pattern analysis, for which Torch and SRS (as primary contractor for the project) received compensation.

39. All of this personal information of Class members was stored in temporary, intermediate computer storage within JetBlue's servers. Through its extensive use of the Internet to run its business and its telephone passenger reservations systems, JetBlue effectively operates an electronic communications service and/or remote computing service with its customers. Indeed, consumers can access and edit personally identifiable information provided to JetBlue by accessing the information through the JetBlue website, by writing to JetBlue or by calling 801-365-2470.

Defendants' Lack of Authorization by or Notice to Plaintiffs

40. Prior to turning over the personal and private data at issue, no Defendant obtained the authorization or consent of passengers necessary under JetBlue's privacy policy or the Electronic Communications Privacy Act, 18 U.S.C. §2701, *et seq.*, that would have permitted the transfer of the personal and private data to a third-party for profiling, testing or any other purpose.

41. Neither JetBlue, Acxiom, Torch nor SRS provided timely notice to JetBlue's customers about Defendants' improper use and manipulation of their data. If the personal and private data at issue were being used to assist with a government project, any party that established a private record system of JetBlue's Passenger Reservation System would have been required first to issue official notice of that system and request the information through a subpoena or other legal process. That did not take place.

The Circumstances Surrounding the Unlawful Sharing of Personal and Private Data Concerning JetBlue's Passengers

42. According to the Department of Homeland Security Privacy Office Report

to the Public on Events Surrounding JetBlue Data Transfer dated February 20, 2004 (the “DHS Report”), following the terrorist attacks of September 11, 2001, representatives of Torch approached the Department of Defense with an unsolicited proposal involving data pattern analysis that was geared towards enhancing the security of military installations throughout the country and potentially internationally. The project “arose out of a desire to prevent attacks on military installations, following the attack on the Pentagon.” Torch proposed that through analysis of personal characteristics of persons who sought access to military installations, a program employing data pattern analysis might be able to predict which persons posed a risk to the security of the military installation. The Torch project later became known as the Base Security Enhancement Program (the “Program”).

43. The Department of Defense was interested in the Program and accordingly added Torch as a subcontractor to an existing contract with SRS for the purpose of performing a limited initial test of the Program. The SRS contract was amended to include a reference to using PNR (erroneously referred to as “P&R”) as a possible data source for the test of the Program. Notably, while Torch developed the idea and method for data analysis, Torch’s proposal depended upon an outside source of data for operational completeness. As a result, Torch sought access to a large, national-level database to be used in assessing its data analysis tool for predicting terrorist behavior.

44. Thereafter, in late 2001 and early 2002, Torch apparently approached numerous federal agencies that operated governmental databases containing personal information for Torch to use in testing its Program. Torch was unsuccessful in obtaining such personal information from the federal agencies.

45. Thus, Torch began to approach commercial sources for the personal

information. Torch began contacting data aggregators and airlines, believing that national airline passenger databases would contain adequate cross-sections of personal characteristics and that airline passenger lists might yield appropriate analytical information.

46. Torch approached other airlines and requested that they provide personal information concerning their passengers. Torch was informed by airline representatives that the airlines would not engage in personal information sharing unless the Department of Transportation and or the Transportation Safety Administration was informed and approved of such data sharing.

47. Frustrated with its inability to obtain the necessary personal information, Torch began to involve members of Congress, asking them to intervene on Torch's behalf with airlines or federal agencies.

48. Torch also contacted the Department of Transportation in April 2002. As a result, Torch held a number of meetings with the Department of Transportation in May and June of 2002, including meetings with representatives of the Department of Transportation Office of Congressional Affairs and Chief Information Officer and several program offices.

49. One such program office with which Torch held at least one meeting was the Transportation Safety Administration office responsible for development of the second-generation Computer Assisted Passenger Prescreening System ("CAPPS II"). According to the DHS Report, "[a]t the time of these meetings, the CAPPS II program was in the most preliminary stages of development, the creation of the program having been announced in March 2002."

50. Torch's conversations and meetings with the Departments of Defense and

Transportation continued through July and August of 2002. Torch has claimed that in July, 2002 it was “given assurance that we would receive the necessary data base being used by CAPPS II contractors in weeks.” However, according to the DHS Report, although the conversations between Torch and the Departments of Defense and Transportation would touch on the development of CAPPS II, the purpose of the conversations was not to assist in CAPPS II development, but to promote the Program, which had no connection to airline routes, rates or services. Indeed, according to the DHS Report, Transportation Safety Administration personnel reportedly stated during the meetings that the development of the Program and the development of CAPPS II should remain separate, and Department of Transportation officials specifically noted that the Program differed from that anticipated for CAPPS II. Apparently, Department of Transportation and Transportation Safety Administration officials endeavored to keep the Program and its potential use of personal information separate from CAPPS II.

51. Following these conversations and meetings, the Department of Transportation and the Transportation Safety Administration agreed to assist Torch in obtaining consent from a national airline to share passenger data for the purposes of the Program.

52. Thereafter, officials with the Transportation Safety Administration contacted JetBlue in New York on Torch’s behalf and began conversations regarding the Program. The Transportation Safety Administration officials represented the overall purpose of the Program to be “the prevention of unauthorized or unwanted entry onto military bases via a variety of forms of entry.”

53. On July 30, 2002, a Transportation Safety Administration official sent JetBlue a written request for JetBlue to supply data concerning its passengers to the Department of Defense for the Program. JetBlue apparently provided this written request for data concerning

its passengers to Acxiom, a data aggregator serving as a contractor for JetBlue, because in August 2002, Acxiom informed Torch that Torch would receive passenger data from JetBlue. JetBlue's passengers, however, were not informed that their personal and private information was going to be transferred to Torch. Nor did JetBlue's passengers consent to the release of their information.

54. Remarkably, JetBlue released its passengers' personal and private information without being compelled to do so by subpoena or other legal process. Rather, in violation of its own privacy policy, JetBlue provided the personal and private information concerning its passengers voluntarily and in response to the Transportation Safety Administration's highly unusual and informal request for JetBlue passengers' personal and private information – information well outside of the norm for the Transportation Safety Administration to request. As the DHS Report concludes “[t]he TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act of 1974” and they acted “outside normal process to facilitate a data transfer, with the primary purpose of the transfer being other than transportation safety.”

55. In September 2002, Acxiom accomplished the transfer of the personal and private data concerning JetBlue's passengers to Torch. That data included, among other things, the passenger's name, address, telephone, and some itinerary-related information. A total of five million records, representing over 1.5 million passengers, were transferred.

56. In October 2002, Torch separately purchased additional data containing personal and private information concerning JetBlue's passengers from Acxiom. That data was then “merged” to create a mega data base of JetBlue passenger information - name, address, gender, own or rent a home, years at residence, economic status, number of adults and children

in family, Social Security number, occupation and number of vehicles owned or leased.

57. Based on the data it received from JetBlue and Acxiom, Torch was able to gather detailed demographic data for over 2 million passengers, or 40% of the passengers in JetBlue's entire data base. Torch then engaged in a data analysis for 200,000 "sample" passengers, grouped into "Younger Affluent" and "Older Affluent" categories, to determine JetBlue's passengers' median age, income, length of residence, home ownership status, gender, number of adults and children in household, and Social Security number grouping - information that arguably has no relationship to military base security, but would be very useful to JetBlue for its own marketing and commercial purposes. JetBlue has not stated that it will not use the results of this analysis for marketing or other purposes.

58. As a result, with the active assistance and agreement of JetBlue and Acxiom and pursuant to a contract between SRS and the Department of Defense, Torch created a customer profiling scheme to "demonstrate that airline passenger and reservation data can be clustered to form groups of conventional travelers" and to show further how this type of profiling, when extended to a more complete data base, can be used to identify "high risk passengers" who can be tagged yellow or red (and thereby subject to either higher pre-flight airlines checks or detention) to "distinguish normal JetBlue's passengers from past terrorists." Torch concluded that its system was workable and that with two additional pieces of information regarding miles traveled, it would be able to "identify and characterize all normal travel patterns" and develop "passenger stability indicators" to assist in the profiling process.

59. According to the DHS Report, however, while Torch used the data containing personal and private information concerning JetBlue's passengers to perform tests of

the Program, the data provided to Torch proved to be “inadequately diverse” because the passenger data represented only certain regions of the country and limited flight patterns.

**The Public Disclosure of the Data Containing
Personal and Private Information Concerning JetBlue’s Passengers**

60. In the Spring of 2003, representatives of Torch appeared at a conference on homeland security technology (the Southeastern Software Engineering Conference sponsored by the National Defense Industrial Association) held in Alabama. Torch gave a presentation at the conference utilizing the data containing personal and private information concerning JetBlue’s passengers and focusing on a “process of analyzing passenger demographics for risk assessment.” The report was titled “Homeland Security Airline Passenger Risk Assessment (the “Conference Report”).

61. As an example of the type of data it had managed to gather from JetBlue and Acxiom, Torch included in the Conference Report the personal details of what it characterized as “anomalous customer data” for at least one passenger, which was then made available on the Internet. The published and publicly available information included the passenger’s address, Social Security number, length of time at current residence, and date of birth. Torch later conceded, in a gross understatement, that the gaffe was “unfortunate.”

62. Further, until at least September 16, 2003, the entirety of the results Torch Concept’s profiling scheme was posted on the Internet website of the Tennessee Valley Chapter of the National Defense Industries Association and thus was publicly available to anyone.

JetBlue Agrees to Share Additional Personal and Private Information

63. In the Summer of 2003, almost a year after the data containing personal and private information concerning JetBlue’s passengers was transferred from Acxiom and after substantial communications between the Transportation Safety Administration and JetBlue, the

Department of Homeland Security disclosed that JetBlue had agreed to participate in testing CAPPS II. On or about September 15, 2003, the Transportation Safety Administration confirmed to privacy advocates that JetBlue would help in the testing of CAPPS II.

64. Nonetheless, there were substantial delays in 2003 in the implementation of CAPPS II testing, including due to the realization by the Transportation Safety Administration that “the JetBlue privacy policy prevented such data sharing, and that JetBlue would need to take affirmative action to amend such policies before any testing began.” As a result, JetBlue’s participation in CAPPS II was delayed significantly.

The Unlawful Disclosure of Data Containing Personal and Private Information Concerning JetBlue’s passengers Transfer is Uncovered and Conceded

65. In the meantime, in September 2003, and apparently in response to JetBlue’s announced participation in CAPPS II testing, members of the public began conducting investigations regarding the transfer of the data containing personal and private information concerning JetBlue’s passengers and were able to obtain on the Internet the Conference Report made by Torch. As a result, there were public accusations against JetBlue regarding that transfer.

66. In response, JetBlue admitted in an interview on or about September 17, 2003 that “we clearly have to review internally this decision and reconsider our policies,” but claimed that no customer information “has been provided for purposes of testing the CAPPS II program currently under design.” Apparently after further examination, JetBlue Chief Executive Officer David Neeleman conceded the improper transfer and released a statement that “[a]lthough I had no knowledge of this data transfer at the time it was made, I accept full responsibility for this action by our company.” Neeleman also acknowledged that the transfer of

the data containing personal and private information concerning JetBlue's passengers had been a violation of JetBlue's own privacy policy.

67. On or about September 18, 2003, JetBlue began to send e-mails to angry passengers, signed by Neeleman in an attempt to distance JetBlue from the controversy and "set the record straight." In the e-mails, JetBlue represented that it has never supplied data to the TSA "or any other government agency" for CAPPS II "or for any other purpose whatsoever." As described herein, that statement was demonstrably false. JetBlue also asserted that "no data files were ever shared with the Department of Defense or any other government agency or contractor" – another clear misrepresentation given the facts represented herein.

68. Thereafter, on September 22, 2003, David Neeleman announced that JetBlue had rescinded its commitment to participate in CAPPS II testing.

69. JetBlue claims that the data generated by Torch "has been destroyed" and that JetBlue is making "every effort" to have the Conference Report removed from the Internet. Nonetheless, there has been no confirmation regarding the fate of the data containing personal and private information concerning JetBlue's passengers or that the destruction of the Conference Report or other Torch data has been completed, or that the monumental (and potentially impossible) effort it would take to eliminate the Conference Report from the Internet has been undertaken or has been successful. Thus, the fate of the data containing personal and private information concerning JetBlue's passengers remains unclear. While JetBlue claims it is "committed to making this right" and will take steps to ensure such a mistake will not happen again, in fact all JetBlue may do is continue to weaken its privacy policy, enabling it to engage in such conduct again. Indeed, it appears that JetBlue already has weakened its privacy policy for just such a purpose. JetBlue's current privacy policy as described on the JetBlue Website

permits JetBlue to “disclose personally identifiable information to government authorities pursuant to a *legal request*, or to third parties pursuant to a subpoena or other legal process.” (Emphasis added.) Accordingly, in response to the public outcry regarding the unauthorized transfer of Plaintiffs’ and other Class members’ personal and private information, JetBlue revamped its privacy policy to permit it to provide its passengers’ personal and private information to any governmental authority that makes a “legal request.” Notably, “legal request” is undefined, but it certainly falls short of requiring a subpoena or other legal process as is specifically required by the privacy policy where non-governmental third parties are involved.

70. While SRS has attempted to distance itself from this controversy, the Program was performed pursuant to a contract between SRS and the Department of Defense. Torch acted as a subcontractor under that contract. As a matter of practice, contractors are responsible for the acts of their subcontractors, especially in the sensitive area of consumer privacy. Thus, SRS did know, or SRS abdicated its responsibilities as a government contractor to know, what its subcontractor was doing, to the detriment and injury of Plaintiffs and members of the Class.

71. As a result of the foregoing, Defendants or their representatives are failing and refusing to abide by and breaching their own agreements with customers and/or applicable standards in the industry, taking actions in violation of federal and state privacy laws, making uniform misleading representations about the data in question (including regarding why it was provided and utilized, the true purpose of the profiling study, what actions have been taken to delete the information from the Internet and what became of the data and any copies thereof), and/or consistently and uniformly omitting material facts as set forth above. Defendants are also

failing and refusing to advise members of the general public of the material facts as set forth above.

72. Members of the general public are particularly vulnerable to such deceptive and fraudulent practices. Most persons possess limited knowledge of the potential for misleading statements and the massive amount of data gathering and profiling that can occur in the travel industry absent adequate protections. In contrast, Defendants possess special expertise in the offering of such products and services. Without having been fully informed of the facts and information described herein, members of the general public may not be aware of their rights and how such conduct violates those rights.

73. Defendants' failures to abide by their legal obligations and their making of false and misleading representations or failing to disclose material facts as set forth above are ongoing and continue to this date.

COUNT I
(VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT –
STORED ELECTRONIC COMMUNICATIONS, 18 U.S.C. § 2701, ET SEQ.)
(AS TO ALL DEFENDANTS)

74. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

75. JetBlue encouraged its customers to provide audibly or electronically personally identifiable information for storage on JetBlue's Passenger Reservation Systems or servers. Plaintiffs and Class members did so, with the express representation and understanding that the information would not be disclosed to another person or entity absent their authorization or consent and in strict adherence to JetBlue's privacy policy.

76. The JetBlue Passenger Reservation Systems or servers used by JetBlue and its passengers to store passenger information constitute an electronic communications service to the public in accordance with 18 U.S.C. § 2510(15).

77. JetBlue knowingly divulged to Torch, SRS and/or Acxiom the contents of Plaintiffs' and Class members' communications while in storage absent the authorization or consent of Plaintiffs or Class members.

78. JetBlue also knowingly exceeded its authorization to access Plaintiffs' and Class members' communications while in electronic storage absent the authorization or consent of Plaintiffs or Class members.

79. Acxiom knowingly divulged to Torch and SRS the contents of Plaintiffs' and Class members' communications while in storage absent the authorization or consent of Plaintiffs or Class members.

80. Acxiom also knowingly exceeded its authorization to access Plaintiffs' and Class members' communications while in electronic storage absent the authorization or consent of Plaintiffs or Class members.

81. Torch and SRS knowingly divulged to the public and to governmental entities as described herein the contents of Plaintiffs' and Class members' communications while in storage absent the authorization or consent of Plaintiffs and Class members.

82. Torch and SRS also obtained unlawful access to the contents of Plaintiffs' and Class members' communications while in storage absent the authorization or consent of Plaintiffs and Class members.

83. Torch and SRS also knowingly exceeded their authorization to access Plaintiffs' and Class members' communications while in electronic storage absent the authorization or consent of Plaintiffs or Class members.

84. Each instance of Defendants' wrongful course of conduct, as set forth above, constitutes a violation of the Electronic Communications Privacy Act, 18 U.S.C. §2701, *et seq.*

85. Plaintiffs and Class members have either suffered actual damages as a result of Defendants' violations of the ECPA as described herein or have suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law as a result of Defendants' violations of the ECPA as described herein.

86. Pursuant to 18 U.S.C. §2707, Plaintiffs and members of the Class are entitled to such preliminary or other equitable or declaratory relief as may be appropriate, at least \$1,000 per Class member in statutory damages, actual and punitive damages, costs and reasonable attorneys' fees, plus disgorgement of any profits Defendants earned as a result of such violations of law.

COUNT II
(BREACH OF CONTRACT)
(AS TO DEFENDANT JET BLUE)

87. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

88. Defendant JetBlue's stated privacy policies, as published on JetBlue's websites or otherwise disclosed to consumers, constitute a self-imposed contractual obligation by and between JetBlue and the consumers with whom it transacted business, including Plaintiffs and members of the Class. The right to maintain personal information pursuant to

Defendant JetBlue's stated privacy policies is an individual right belonging to Plaintiffs and each member of the Class.

89. Plaintiffs and each member of the Class fully performed their respective obligations under their respective contracts with JetBlue.

90. JetBlue breached its contracts with Plaintiffs and the other members of the Class in that, contrary to its stated privacy policies, JetBlue disclosed personal information concerning Plaintiffs and the members of the Class to third-parties without first obtaining the required consent of Plaintiffs and the members of the Class.

91. As a direct and proximate result of Defendant JetBlue's breaches, which injured Plaintiffs and the members of the Class, JetBlue is liable to Plaintiffs and the other members of the Class for actual damages in an amount to be determined at trial.

COUNT III
(VIOLATION OF NEW YORK GENERAL BUSINESS LAW
SECTION 349 AND OTHER SIMILAR STATE STATUTES)
(AS TO ALL DEFENDANTS)

92. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

93. Defendants were aware that JetBlue's passengers provided personally identifiable information subject to JetBlue's privacy policy, *i.e.*, the data containing personal and private information concerning JetBlue's passengers. The privacy policy provided that personal information such as the data containing personal and private information concerning JetBlue's passengers gathered by Defendant JetBlue would not be disclosed to third parties. Plaintiffs and other Class members relied upon those representations and assurances when choosing to purchase air transportation from JetBlue.

94. Defendants engaged in unfair or deceptive acts and practices by

knowingly and surreptitiously conspiring to obtain and, thereafter, obtaining, maintaining and manipulating Plaintiffs and Class members' data containing personal and private information, which they knew or should have known was received in direct violation of Defendant JetBlue's privacy policy, in violation of New York General Business Law § 349, *et seq.* or similar state deceptive state practice acts or statutes.

95. Defendants actions had no connection with airline routes, rates or services.

96. Defendants used the data containing personal and private information concerning JetBlue's passengers provided by Defendant JetBlue for their own commercial benefit absent the authorization or consent of Plaintiffs or any other Class member.

97. The conduct described above constitutes unfair or deceptive trade practices predominantly and substantially affecting the conduct of trade or commerce throughout the United States in violation of the New York General Business Law § 349, *et seq.*, and other similar state statutes prohibiting unfair and deceptive acts and practices including:

Alaska:	Alaska Stat. §45-50-471, <i>et seq.</i>
Arizona:	Ariz. Rev. Stat. §44-1522(A), <i>et seq.</i>
Arkansas:	Ark. Code Ann. 4-88-101, <i>et seq.</i>
California:	Cal. Civ. Code §§1780 - 1784, Business and Profession Code §17200, <i>et seq.</i> , §17500, <i>et seq.</i>
Connecticut:	Conn. Gen. Stat. Ann. §§42-110a - 42-110g, <i>et seq.</i>
Colorado:	Col. Rev. Stat. §§6-1-101 - 6-1-114, <i>et seq.</i>
Delaware:	6 Del. Code Ann. §§2511 - 2537, <i>et seq.</i>
District of Columbia:	D.C. Code Ann. §§28-3801 - 28-3819, <i>et seq.</i>
Florida:	Fla. Stat. Ann. §§501.201 - 501.213, <i>et seq.</i>

Georgia:	Ga. Stat. §10-1-393(b)(5), (7), <i>et seq.</i>
Hawaii:	Hawaii Rev. L. §§480-1 - 480-24, <i>et seq.</i>
Idaho:	Idaho Code §§48-601 - 48-619, <i>et seq.</i>
Illinois:	815 ILCS 505/2, <i>et seq.</i>
Indiana:	Ind. Code §24-5-0.5-3(a)(1), (2), <i>et seq.</i>
Iowa:	Iowa Code §714.16, <i>et seq.</i>
Kansas:	Kan. Gen.Stat. Ann. §§50-623 - 50-644, <i>et seq.</i>
Kentucky:	Ky. Rev. Stat. Ann. §§367.110 - 367.990, <i>et seq.</i>
Louisiana:	La. Rev. Stat. Ann. §§13:1401 - 13:1418, <i>et seq.</i>
Maine:	Me. Rev. Stat. Ann. §§206 - 214, <i>et seq.</i>
Maryland:	Md. Code Ann. §13-501, <i>et seq.</i>
Massachusetts:	Mass. Gen. L. Ann. Ch. 93A. §§1 - 11, <i>et seq.</i>
Michigan:	Mich. Stat. Ann. §19.418(B), <i>et seq.</i>
Minnesota:	Minn. Stat. Ann. §§325D.09 - 325D.16, <i>et seq.</i>
Mississippi:	Miss. Code §75-24-5(1), (2)(e) & (g), <i>et seq.</i>
Missouri:	Mo. Ann. Stat. §§407.010 - 407.701, <i>et seq.</i>
Montana:	Mont. Rev. Code Ann. §§30-14-101 - 30-14-224, <i>et seq.</i>
Nebraska:	Neb. Rev. Code §§59-1501 - 59-1623, <i>et seq.</i>
Nevada:	Nev. Rev. Stat. §§590A.010 - 590A.280, <i>et seq.</i>
New Hampshire:	N.H. Rev. Stat. Ann. §358-A:2, <i>et seq.</i>
New Jersey:	N.J. Stat. Ann. §§56:8-1 - 56:8-24, <i>et seq.</i>
New Mexico:	N.M. Stat. Ann. §57-12-10, <i>et seq.</i>

North Carolina:	N.C. Gen. Stat. §§75-1 - 75-56, <i>et seq.</i>
North Dakota:	N.D. Cent. Code §51-15-02, <i>et seq.</i>
Ohio:	Ohio Rev. Code Ann. §1345, <i>et seq.</i>
Oklahoma:	Okla. Stat. Tit. 15 §753, <i>et seq.</i>
Oregon:	Ore. Rev. Stat. §§646.605 - 646.642, <i>et seq.</i>
Pennsylvania:	73 Pa. Stat. §201, <i>et seq.</i>
Rhode Island:	R.I. Rev. L. Ann. §§6-13.1-1 - 6-13.1-11, <i>et seq.</i>
South Carolina	S.C. Code §39-5-20(a), <i>et seq.</i>
South Dakota:	S.D. Comp. L. §§37-24-1 - 37-24-35, <i>et seq.</i>
Tennessee:	Tenn. Code Ann. §47-18-101, <i>et seq.</i>
Texas:	Tex. Rev. Civ. Stat. §§17.41 - 17.63, <i>et seq.</i>
Utah:	Utah Code Ann. §13-11-19, <i>et seq.</i>
Virginia	Va. Code §59.1-200(A)(5)-(7), (14), <i>et seq.</i>
Vermont:	Vt. Stat. Ann. §§2451 - 2462, <i>et seq.</i>
Washington:	RCW §19-86-010, <i>et seq.</i>
West Virginia:	W. Va. Code Ann. §46A-6-104
Wisconsin:	Wis. Stat. Ann. §100.18, <i>et seq.</i>
Wyoming	Wyo. Stat. §40-12-105(a)(3), (xv), <i>et seq.</i>

98. As a direct and proximate result of this alleged conduct, Plaintiffs and members of the Class have suffered actual damages and request an award of damages as against all Defendants, as authorized by such statutes. In the alternative, Plaintiffs have suffered an irreparable injury for which there is no adequate remedy at law as a result of Defendants' conduct, and Plaintiffs are entitled to appropriate temporary and permanent injunctive relief as a

result, as authorized by such statutes. Plaintiffs and members of the Class further are entitled to such preliminary or other relief as may be provided by such statutes, including statutory damages, punitive damages, costs and reasonable attorneys' fees, plus disgorgement of any profits Defendants earned as a result of such violations of law.

COUNT IV
(TRESPASS TO PROPERTY)
(AS TO ALL DEFENDANTS)

99. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

100. Either directly or by aiding and abetting and/or conspiring to do so as described herein, Defendants transferred and/or used Plaintiffs' and the Class members' personal property, *i.e.*, the data containing personal and private information concerning JetBlue's passengers contained in electronic storage.

101. As a direct and proximate result of this alleged conduct, Plaintiffs and members of the Class have suffered actual damages and request an award of damages as against all Defendants. In the alternative, Plaintiffs have suffered an irreparable injury for which there is no adequate remedy at law as a result of Defendants' conduct, and Plaintiffs are entitled to appropriate temporary and permanent injunctive relief as a result. Pursuant to the common law, Plaintiffs and members of the Class are entitled to such other damages, including punitive damages, as provided by law.

COUNT V
(INVASION OF PRIVACY)
(AS TO ALL DEFENDANTS)

102. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

103. Defendants have, either directly or by aiding, abetting and/or conspiring to do so, knowingly disclosed, exploited, misappropriated and/or engaged in widespread commercial usage of private and sensitive information concerning the Plaintiffs' and the Class members' personal affairs, *i.e.*, the data containing personal and private information concerning JetBlue's passengers, without the knowledge, authorization, or beyond the consent of Plaintiffs and members of the Class. Such conduct constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class members' privacy.

104. Because Plaintiffs and the Class members did not voluntarily authorize the disclosure of the data containing personal and private information concerning JetBlue's passengers, such information was misappropriated.

105. As a direct and proximate result of this alleged conduct, Plaintiffs and members of the Class have suffered actual damages and request an award of damages as against all Defendants. In the alternative, Plaintiffs have suffered an irreparable injury for which there is no adequate remedy at law as a result of Defendants' conduct, and Plaintiffs are entitled to appropriate temporary and permanent injunctive relief as a result. In addition, Plaintiffs and members of the Class are entitled to such other damages, including punitive damages, as may be provided by law.

COUNT VI
(UNJUST ENRICHMENT)
(AS TO ALL DEFENDANTS)

106. Plaintiffs repeat and reallege the allegations contained in Paragraphs 1-98 above, as if fully set forth herein.

107. Defendants have wrongfully and unlawfully enriched themselves to

Plaintiffs' and the Class members' detriment by engaging, and continuing to engage, in the above-described wrongful course of conduct for their own commercial benefit and enrichment.

108. Defendants' continued use, enjoyment, and retention of these wrongfully and unlawfully received funds or other benefits violates fundamental principles of justice, equity, and good conscience and thus constitutes unjust enrichment.

109. As a direct and proximate result of defendants' above-described wrongful course of conduct, Plaintiffs and members of the Class have suffered actual damages and request an award of damages as against all Defendants. In addition, Plaintiffs and members of the Class are entitled to such punitive damages and disgorgement of any profits Defendants earned as may be provided by law.

COUNT VII
(DECLARATORY JUDGMENT)

110. Plaintiffs repeat and reallege the allegations contained above, as if fully set forth herein.

111. Plaintiffs and the members of the Class members entitled to a declaratory judgment that by commission of the acts and omissions alleged herein, defendants have violated the Electronic Communications Privacy Act – Stored Electronic Communications, 18 U.S.C. §2701 *et seq.*, New York General Business Law 349, *et seq.* and the similar state statutes listed, above, and/or Plaintiffs' and Class members' common law rights against trespass to property, invasion of privacy, breach of contract and Defendants' unjust enrichment.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully requests that the Court enter judgment in their favor and against Defendants:

- A. Determining that the action is a proper class action maintainable under Fed. R. Civ. P. 23; certifying an appropriate Class and certifying Plaintiffs as Class Representatives;
- B. Ordering the temporary and preliminary off-site storage, under strict independent monitoring, of all information collected and/or shared as a result of Defendants' wrongful conduct described herein in order to preserve the *status quo* pending the Court's resolution of the issues raised by this Complaint;
- C. Ordering a temporary and preliminary asset freeze or constructive trust on all monies wrongfully obtained, and all profits wrongfully derived, as a result of the conduct alleged in this Complaint in order to preserve the *status quo* pending the Court's resolution of the issues raised by this Complaint;
- D. Declaring the acts and practices complained of herein to be in violation of the statutory and common laws set forth above;
- E. Enjoining and restraining the Defendants from any further acts in violation of the statutory and common laws set forth above;
- F. Directing the Defendants to take such affirmative steps as are necessary to ensure both that the causes and effects of their unlawful information-handling acts and practices are eliminated and no longer continue and that all Class members are specifically notified of JetBlue's information-handling acts and practices and the existence and availability of a remedy to correct the illegal

activities set forth above. At a minimum, such affirmative steps must include: i) ordering the Defendants to conduct a corrective advertising and information campaign advising consumers whose electronically stored personal information has already been transferred and/or accessed how to determine if their information was improperly transferred and/or accessed, and ii) ordering the destruction and/or purging, under court monitoring, of all personally identifiable information transferred by JetBlue to any person a result of Defendants' wrongful conduct described herein.

- G. Awarding Plaintiffs and the Class any and all amounts owing to them under the statutes of the United States or any state therein as set forth above;
- H. Awarding Plaintiffs and the Class any and all amounts owing to them under state deceptive and unfair trade practice statutes set forth above.
- I. Awarding Plaintiffs and each Class member their actual and compensatory damages for violations of the statutes of the United States set forth above and violations of their right to be free from trespass to property, invasion of their privacy;
- J. Awarding Plaintiffs and members of the Class punitive damages;
- K. Directing Defendants to disgorge all monies wrongfully obtained as a result of the conduct alleged in this Complaint and awarding

to Plaintiffs and the Class members all profits derived or monies saved as a result of the unlawful acts and practices alleged herein;

- L. Awarding Plaintiffs and the Class members the costs of this action, together with reasonable attorneys' fees;
- M. Awarding Plaintiffs and members of the Class pre- and post-judgment interest; and
- N. Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs hereby demand a trial by jury in this action of all issues so triable.

Dated: April 30, 2004
New York, New York

CAULEY, GELLER, BOWMAN & RUDMAN, LLP

By: /s/ Robert M. Rothman

Robert M. Rothman (RR 6090)
Samuel H. Rudman (SR 7957)
David A. Rosenfeld (DR 7564)
200 Broadhollow Road, Suite 406
Melville, NY 11747
Telephone: (631) 367-7100

MILBERG WEISS BERSHAD HYNES & LERACH LLP

Michael M. Buchman (MMB-1172)
J. Douglas Richards (JDR-6038)
One Pennsylvania Plaza
New York, New York 10119-0165
Telephone: (212) 594-5300

Plaintiffs' Co-Lead Counsel

KIRBY McINERNEY & SQUIRE

Ira Michael Press (IP 5313)
Mark A. Strauss (MS 2288)
830 Third Avenue, 10th Floor
New York, NY 10022

HOLZER HOLZER & CANNON

Christi A. Cannon
1117 Perimeter Center West, Suite E-107
Atlanta, GA 30338

WITES & KAPETAN, P.A.

Marc Wites
1701 West Hillsboro Blvd.
Suite 305
Deerfield Beach, FL 33442

**WECHSLER HARWOOD HALEBIAN &
FEFFER LLP**

Robert I Harwood
488 Madison Avenue
New York, NY 10022

SCHIFFRIN & BARROWAY, LLP

Marc A. Topaz
Three Bala Plaza East, Suite 500
Bala Cynwyd, PA 19004

REINHARDT WENDORF & BLANCHFIELD

Garrett D. Blanchfield, Jr.
1250 East First National Bank Building
332 Minnesota Street
S. Paul, Minnesota 55101

RABIN MURRAY & FRANK LLP

Brian P. Murray
275 Madison Avenue
34th Floor
New York, NY 10016

THE BRUALDI LAW FIRM

Richard B. Brualdi
29 Broadway, Suite 1515
New York, NY 10006

SHALOV STONE & BONNER LLP

Lee S. Shalov
485 Seventh Avenue, Suite 1000
New York, NY 10018

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

Richard A. Lockridge
Karen Hanson Riebel
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401

SPECTOR ROSEMAN & KODROFF

Jeffrey J. Corrigan
William G. Caldes
1818 Market Street
Suite 2500
Philadelphia, PA 19103

Members of the Executive Committee